REMARKS

Applicant gratefully acknowledges the courtesy of the Examiner in granting an interview to Applicant's representative David Zviel, registration number 41,392, on 15 June 2004. In the interview, the Examiner and Applicant's representative discussed US Patent 5,426,700 and Claim 44 as described in more detail below. The discussion centered around the number of keys fed to the system, punctuation of the "determining" step, feeding the device an invalid content key as specified in the "wherein" clause, and the significance of "providing a device to be analyzed".

Applicant has carefully studied the outstanding Official Action. The present response is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Claims 44 and 46 - 50 are pending in the application before the present amendment.

Claims 44, 46 and 48 - 50 stand rejected under 35 USC 102 as being unpatentable over US Patent 5,426,700 to Berson.

Berson describes a method and apparatus to authenticate documents belonging to selected groups of classes of documents. A device is sent an encryption key encrypted with one of a number of group keys corresponding to particular classes, not all of which match document content. The applicability of each key is determined, by determining if the decryption of a document using the key matches an unencrypted version of the document (col. 6, line 52 - col. 7 line 4; col. 7 lines 29 - 37; col. 8 lines 37 - 65).

Preferred embodiments of the present invention, by contrast, comprise a method for black box analysis of a device capable of accessing protected content, the method comprising, inter-alia, "identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result" (claim 44). Further support for Applicant's argument that preferred embodiment of the present invention are directed to black box analysis of a device is found, inter-alia, on page 4, lines 4 - 7 and 22 - 24: "In a

preferred embodiment of the present invention, an improved key distribution system is provided, the improved key distribution system having the following features: ... 6. Black box analysis, that is, analysis of a device to determine which secrets it knows by challenge and response without reverse engineering of the device, is relatively easy, so that analysis of pirate devices is relatively easy."

Applicant also respectfully points out that in further contrast to Berson, in preferred embodiments of the present invention content keys are provided to a device; both a valid content key encrypted with some group keys, and an invalid content key encrypted with some other group key. If the device returns null or erroneous content (refer to pages 20 and 21 of the specification for a discussion of the meanings of the terms "null" and "erroneous"), then we can deduce what group key or keys the device "knows".

Furthermore, it is respectfully pointed out that the present invention, as claimed, for example, in independent claim 44, solves a problem of black box analysis of a device capable of accessing protected content.

Berson, by contrast, describes "a reliable document verification system and, in particular, relates to a reliable document verification system using a public key cryptosystem." (col. 1 lines 6 - 9, inter-alia). That is, Berson relates to authentication of a document.

Thus, the problem solved by the present invention, as claimed, for example, in independent claim 44 is very different from that solved by Berson.

Nevertheless, in order to place the application in better condition for allowance, claim 44 has been amended to clarify the differences between the present invention and Berson. Support for the amendments is found, inter-alia, on page 20 of the specification.

Changes have also been introduced to the line spacing in claim 44 in order to clarify the wording of claim 44. These changes are not believed to affect patentability of claim 44.

In light of the above discussion, claim 44 is deemed allowable.

Claims 46 and 48 - 50 depend from claim 44 and recite additional patentable subject matter.

Claims 46 and 48 - 50 are therefore deemed allowable.

Claim 47 stands rejected under 35 USC 103 as being unpatentable over Berson and further in view of US Patent 5,309,516 to Takaragi et al.

Takaragi et al. describes a method and system which permit group cipher communication from a desired terminal to a number of desired terminals while ensuring security. A plurality of secret values (master keys) which are common to a predetermined subset of IC cards are stored in an IC card. Takaragi describes an iterative process whereby it is determined whether of not a particular master key is designated for a single office or is one of a larger set (col. 9 - lines 15 - 62).

Applicant respectfully submits that the motivation to combine Berson with Takaragi et al. suggested by the Examiner is based on hindsight. Neither Berson nor Takaragi et al. provide said motivation.

In any event, claim 47 is indirectly dependent from claim 44 and recites additional patentable subject matter.

Claim 47 is therefore deemed allowable, both with reference to the above discussion, and with reference to the discussion of the allowability of claim 44.

New claims 67 - 80 have been added. New claims 67 - 80 are supported, inter-alia by pages 4 - 5 and 20 of the specification.

Applicant has carefully studied the other prior art of record including:

US Patent 4,771,458 to Citta et al.;

US Patent 4,926,475 to Spiotta et al.;

US Patent 5,592,552 to Fiat;

US Patent 5,661,803 to Cordery et al.;

US Patent 5,812,666 to Baker et al.;

US Patent 6,035,405 to Gage et al.;

US Patent 6,195,751 to Caronni et al.;

US Patent 6,262,435 to Dondeti et al.; and

US Patent 6,530,020 to Aoki et al.

US Patent 4,771,458 to Citta et al. describes a method of operating a data packet communication system including encrypting a first data packet with a

global encryption key, encrypting an addressed data packet including a subscriber address with an address encryption key, transmitting said data packets to subscriber terminals, and causing subscriber terminals to search among a plurality of stored global decryption keys for a decryption key corresponding to said global encryption key.

US Patent 4,926,475 to Spiotta et al. describes an encryption key monitoring system for periodically testing an encryption key of at least one of a plurality of encryption circuit means, each of said encryption circuit means generating encrypted data from plain data using an encryption key.

US Patent 5,592,552 to Fiat describes a selective broadcasting method operative to transmit a plurality of message data signals to a corresponding plurality of subscriber subsets within a set of subscribers.

US Patent 5,661,803 to Cordery et al. describes a method of token verification in a key management system providing a logical device identifier and a master key created in a logical security domain to a transaction evidencing device. The method creates a master key record in a key verification box, securely stores the master key record in a key management system archive, and produces in the transaction evidencing device evidence in the logical security domain of transaction information integrity.

US Patent 5,812,666 to Baker et al. describes a key management system for generating, distributing and managing cryptographic keys used by an information transaction system that employs cryptographic means to produce evidence of information integrity.

US Patent 6,035,405 to Gage et al. describes a method for securely adding a new end station to a local area network (LAN) segmented into a number of virtual local area networks (VLANs).

US Patent 6,195,751 to Caronni et al. describes a system for secure multicast including a plurality of participants that can send and receive multicast messages.

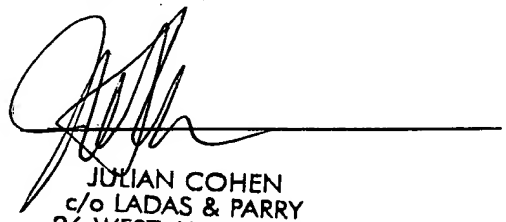
US Patent 6,263,435 to Dondeti et al. describes a tree structure and method for managing membership in a multicast group providing scalability and security from internal attacks.

US Patent 6,530,020 to Aoki et al. describes an encryption process operation of a plain text by an arbitrary member belonging to the group, and a decryption process operation of cryptogram information which can be executed by employing a combination key made from a group public key and a group secret key.

Applicant finds that the present invention as claimed is neither described nor suggested in the prior art of record, taken either individually or in combination.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,



JULIAN COHEN
c/o LADAS & PARRY
26 WEST 61st STREET
NEW YORK, N. Y. 10023
Reg. No. 20302 (212) 708-1887